INTERNET

MĂSURI DE SIGURANȚĂ ÎN UTILIZAREA INTERNETULUI.

PERICOLELE INTERNETULUI

Internetul oferă surse importante de informații și servicii variate, dar nu este atât de sigur pe cât am crede.

Cele mai mari pericole la care ne expunem sunt:

- Descărcarea de programe cu rol distructiv (viruși);
- Expunerea la conținuturi nepotrivite;
- Furtul de date personale sau identitate virtuală;
- Trafic de persoane.

MALWARE

Software-ul rău intenționat sau dăunător, numit adesea ***malware***, cuvânt englez construit din sintagma ***mal***icious soft***ware***, este un tip de software proiectat intenționat pentru deteriorarea unui computer sau infiltrarea în el, sau/și deteriorarea ori infiltrarea în întregi rețele de computere, fără consimțământul proprietarului respectiv.

MALWARE

Programele malware variază în funcție de scopul lor, de modul în care infectează un computer, de modul în care se repetă și de daunele sau riscurile de securitate pe care le prezintă.

Malware este prezent în toate sistemele de operare: Windows, Mac OS, Unix-like, Linux sau Android. Windows este în continuare principalul sistem de operare pentru majoritatea utilizatorilor și, prin urmare, va fi întotdeauna principala țintă pentru malware.

VIRUȘII INFORMATICI

VIRUS este abrevierea de la ***V***ital ***I***nformation ***R***esources ***U***nder ***S***iege (Resurse informaționale vitale sub asediu).

Virușii informatici sunt programe cu caracter distructiv, care se pot instala singure, fără voia utilizatorului.

VIRUȘII INFORMATICI

Aceștia infectează sectorul de boot al hard drive-ului și fișierele executabile și mută datele în cadrul acestui sector, sau îl supra-aglomerează cu informații. Cel mai adesea, virusul informatic se răspândește prin partajarea de software sau fișiere între computere și prin e-mail-uri trimise în masă.

VIERME INFORMATIC (WORM)

Viermele informatic este un program de calculator independent și autonom care se poate replica pentru a se răspândi în alte fișiere de pe calculatoare. De obicei viermii utilizează o rețea de calculatoare pentru a se răspândi, bazându-se pe breșe de securitate ale computerului țintă.

Viermii provoacă daune rețelei, prin ***creșterea traficului în rețea și consumarea lățimii de bandă***. Spre deosebire de virus, un vierme nu are nevoie să se atașeze de un program existent pe calculator.

CAL TROIAN (TROJAN)

Un ***cal troian*** sau simplu troian, este un program malware care se deghizează în software legitim.

Termenul derivă din mitul clasic al calului troian.

Spre deosebire de virușii de calculator și viermi, în general ***troienii nu încearcă să se infiltreze în alte fișiere ale unui calculator sau să se propage în rețea***.

CAL TROIAN (TROJAN)

Un troian pentru computere este una dintre cele mai periculoase forme de malware, datorită capacității sale de a înșela utilizatorii de intenția sa adevărată. După ce un troian a infectat un computer, acesta se activează și ***poate fi folosit pentru a obține accesul la un computer și a sustrage date sensibile***.

Exemple de troiani: Poweliks, Flame.A, FakeAV, Startpage.AABI, Qhost, OlympicGames, Ransom.IcePol, Android.Geinimi.A.

SPYWARE

Este un program spion folosit pentru a ***colecta informații personale*** (nume de autentificare, parole, date personale, informații despre obiceiurile de navigare).

Aceste informații sunt folosite în scopuri de marketing și promovare, conducând implicit și la mărirea numărului de spam-uri.

De obicei, spyware este inclus în programele de tip shareware (software-ul proprietar care este furnizat gratuit pentru o perioadă limitată, cu restricții de funcționalitate, disponibilitate sau comoditate în utilizare).

ADWARE

Adware afișează anunțuri pe computer. Este cotat ca fiind cel mai puțin periculos dar și cel mai profitabil ***grayware*** (termen generic care se referă la aplicații sau fișiere neclasificate drept viruși sau troieni, dar care pot afecta în mod negativ performanțele calculatoarele sau a rețelelor).

Această formă de malware este adesea instalată împreună cu alte aplicații utile, fără știrea utilizatorului și rămâne activ după dezinstalarea acestuia.

RANSOMWARE

Cunsocut și sub numele de „***cryptovirus***”, „***cryptotroian***” sau „***cryptoworm***”, ransomware este un tip de software rău intenționat care blochează accesul la calculator și cere plata unei recompense.

Unele versiuni de ransomware pretind că plata ar trebui efectuată pentru a evita pedepsirea de către o autoritate guvernamentală (FBI sau o agenție locală), sau că acesta este singurul mod de a decripta datele criptate

RANSOMWARE

Primele variante ale acestui tip de malware au fost lansate în Rusia.

Ransomware se poate răspândi prin atașamentele de e-mail, software infectat și site-uri compromise.

Cele mai cunoscute exemple de ransomware sunt WannaCry, CryptoLocker, Locky și FBI MoneyPak.

PROTECȚIA ANTI-MALWARE

Având în vedere diversitatea tipurilor de amenințări se recomandă utilizarea unei suite de programe de securitate care să conțină un ***firewall*** și un ***antivirus***.

Firewallul este o componentă software sau hardware care filtrează în permanență transmisiile de date dintre computer și Internet, pentru a ține la distanță hackerii și conținutul malware.

Un program ***antivirus*** are rolul de a găsi și de a elimina malware și de a proteja computerul de aceștia.

PROGRAMELE ANTIVIRUS

Un program ***antivirus*** are rolul de a găsi și de a elimina malware și de a proteja computerul de aceștia.

Printre cele mai cunoscute și utilizate programe antivirus se pot enumera: Microsoft Security Essentials, Avira, Eset Nod32, Norton Antivirus, Kaspersky, Avast, Bitdefender etc.

SECURITATEA INFORMATICĂ

O soluție completă de securitate trebuie să ofere:

1. Scanarea fișierelor la accesarea acestora;
2. Scanarea fișierelor la cerere;
3. Analiza site-urilor web vizitate;
4. Analiza comportamentului programelor rulate;
5. Analiza vulnerabilității programelor instalate pe calculator.